1. Шахриманьян И. К. Психологические основы отдельных следственных действий. М., 1972. 112 с.

2. Севостьянов Р. А. «Признание вины» и «раскаяние» как критерии исправления осужденного: теоретические аспекты // Вестн. Саратов. гос. юрид. академии. 2017. № 1. С. 177–181.

3. Новиков С. А. Показания обвиняемого в современном уголовном процессе России. СПб., 2004. 240 с.

4. Полстовалов О. В. Криминалистическая конфликтология: современные нравственные и психологические проблемы : монография. Уфа : РИО БашГУ, 2002. 152 с.

5. Назаров А. Д. Следственные ошибки в досудебных стадиях уголовного процесса : учеб. пособие. Красноярск : КГУ, 2000. 323 с.

УДК 343.98

Д. Б. Санакоев
доцент кафедры оперативно-розыскной деятельности и специальной техники Днепропетровского государственного университета внутренних дел (Украина), кандидат юридических наук, доцент

ПРОТИВОДЕЙСТВИЕ НЕПРАВОМЕРНОМУ КОНТЕНТУ: МЕЖДУНАРОДНАЯ ПРАКТИКА И ПУТИ ЕЕ РЕАЛИЗАЦИИ

Стремительное развитие киберпреступности требует постоянного совершенствования существующих и выработки новых мер противодействия, в частности — осуществления контроля доступа к распространению неправомерного веб-контента спецподразделениями киберполиции и его межрегиональными подразделениями.

В этой статье предметом анализа являются вопросы фильтрации информационного наполнения веб-сайтов, задачи которой ограничиваются запретом доступа к определенным сайтам и применением схем, его усложняющих, с целью: 1) защиты граждан от таких преступлений (правонарушений), от ущерба, наносимого им постоянным пребыванием вредящей информации в Интернете (в частности, детская сексуальная эксплуатация); 2) ограничение свободного использования определенных высказываний; 3) введение запрета на доступ к информационному наполнению политического содержания; 4) защита экономических интересов, что касается преимущественно мультимедийного контента, распространяющегося без разрешения владельцев авторских прав с использованием различных приложений, например голосовой связи через IP-протокол (VOIP).

Там, где государство жестко контролирует контент обычных СМИ, вводятся и строгие ограничения по законодательному запрету размещения в веб-сети определенных сведений, блокирование доступа к отдельным сайтам и контроль доступа пользователей. Жесткий контроль характерен преимущественно для стран Восточной и Центральной Азии, Ближнего Востока и Северной Африки [1; 2]. Такие государства проявляют наибольшую активность по ограничению доступа к интерактивной информации, однако в ряде других стран запрещен доступ к сайтам определенного содержания, например с детской порнографией или веб-страниц с вредоносным программным обеспечением. По крайней мере, вопрос о введении запретов там рассматривается, причем с использованием технологий, применяемых для ограничения свободы слова в Интернете [3, с. 207–212]:

1. Технология фильтрации. Для фильтрации web-контента предлагаются два разных подхода. Первый — провайдер предоставляет доступ к Интернету только пользователям, которые, по действующему законодательству, должны (или им рекомендуется) применять механизмы фильтрации; второй — инфраструктура фильтрации устанавливается в пунктах стратегического назначения, служащих связующим звеном между национальными сетями и международной магистральной сетью, как разновидность виртуальной границы. Второй подход предпочитают страны с уже развернутой телекоммуникационной сетью или с существующим государственным надзором и контролем, где изначально необходимость применения фильтрации web-контента так или иначе была очевидной (например, китайская система «Great Firewall» («Золотой щит»).

1.1. Блокировка по IP-адресу. Метод предусматривает введение запрета на доступ к определенным IP-адресам, включенным в список запрещенных. Это наиболее простая и примитивная в использовании технология. Она не требует значительных капиталовложений в специализированное оборудование (ведь ее функции ограничиваются проверкой заголовков TCP/IP) и практически не влияет на производительность сети.

1.2. Блокировка по домену. Первичная форма методики блокирования трансформировалась в метод блокировки с использованием не IP-адреса, а имени домена в качестве критерия фильтрации. Этот подход повысил избирательность фильтрации, но не повлиял на законопослушные домены, пользующиеся услугами одного и того же хостинг-провайдера и списками запрещенных IP-адресов.

Одной из стран, отдающих предпочтение именно этому методу, является Германия, где принят закон [4], по которому предусмотрена возможность интернет-провайдеров блокировать DNS-запросы, касающиеся имен доменов, включенных правоохранительными органами в специальный, постоянно обновляющийся, список с тем, чтобы блокировать доступ к сайтам с детской порнографией в максимально сжатые сроки после их идентификации. Такие страны, как Австралия, Великобритания и Норвегия, также применяют блокирование по DNS. В случаях, когда пользователь запрашивает IP-адрес, внесенный в «черный список» имен доменов, DNS-сервер возвращает адрес на статическую web-страницу с предупреждением о том, чтобы сторона запроса обратила внимание на информационное наполнение интересующей ее страницы (например, kid.telenor.net). С технической точки зрения избежать такой блокировки достаточно просто: достаточно лишь изменить конфигурацию компьютера так, чтобы он обращался к DNS-серверу другой страны (например, к OpenDNS) (например, www.opendns.com).

1.3. Блокировка по URL. Более эффективным методом блокировки является проверка полного адреса запрашиваемого ресурса в сети (URL) и предоставление доступа или отказ в нем на основании более сложных правил. Это позволяет блокировать доступ только к определенным частям веб-сайта. С технической точки зрения такой метод фильтрации, как правило, осуществляется путем установления прокси-сервера, который может быть и прозрачным, и непрозрачным, но обязательным для применения. Прокси-сервер блокирует все попытки получить веб-контент, минуя его. Поскольку такой сервер становится единственным источником веб-контента для всех пользователей, можно легко создать правила, контролировать режим его работы в зависимости от запрашиваемого домена, страницы или даже параметров информации. Например, можно блокировать интерактивные запросы, в которых содержатся ключевые слова из «черного списка» и выполняются через Google или другую поисковую систему, поскольку условия поиска будут отображаться как параметры «get» («Отправить») в URL, что дает доступ к полученным результатам. Эта технология используется отдельными странами для массивной фильтрации веб-контента, в том числе с применением программ SmartFilter и Fortinet Fortiguard от компании McAfee.

1.4. Блокировка по ключевым словам, или пакетная фильтрация. При ее использовании блокируется объем контента, больший необходимого. Так, может блокироваться доступ к учебным

материалам по репродуктивной биологии, ведь информационное наполнение по этим темам обычно содержит слова, которые ассоциируются с порнографией. Такую информацию, как правило, используют в сочетании с «белыми списками» доменов, вызывающих доверие, где ограничения по ключевым словам не производятся. Однако этот метод требует слишком много ресурсов, из-за чего анализ информационного трафика становится экономически и технически нецелесообразным. В то же время на рынке компьютерных технологий существует значительное количество различных коммерческих решений по кодированию информации для нейтрализации механизмов контроля, в частности Tor и FreeNet, которые способны скрыть определенные действия пользователя так, чтобы доступной была только информация о соединении с узлом, принадлежащим этим сетям, однако конкретных сведений о полученном контенте у контролирующих подразделений не будет [3, с. 209].

1.5. Изменение результатов поиска. Как вариант, вместо (или кроме) механизмов блокировки доступа к информации можно прописать команду удалять противозаконный или нежелательный контент из результатов поиска в Интернете. Как правило, такие сведения также фильтруют с помощью некоторых указанных нами методов, а цель удаления такого контента заключается в том, чтобы скрыть сам факт существования какой-либо цензуры.

2. Прозрачность и информация конечного пользователя. Следует различать не только методы проверки контента, но и страны, которые пытаются обеспечить прозрачность механизмов фильтрации и контроля, сообщают пользователю о том, что запрашиваемый ресурс запрещен, или предлагают изменить критерии фильтрации, а также страны, где маршруты запроса или параметры фильтрации меняются без объяснений.

Противоположный подход наблюдаем в таких странах, как Саудовская Аравия, где, несмотря на применение фильтрации к значительному по объемам контенту, пользователю, кроме сообщения о причинах блокировки информации, предлагаются механизмы обращения в государственные органы для пересмотра правил запретов. В любом случае полного «черного списка» ресурсов, подлежащих фильтрации, не существует ни в открытом, ни в ограниченном доступе для спецподразделений киберполиции, как следствие — систему часто взламывают с конкретной целью, например, для фильтрации сексуальных снимков несовершеннолетних или иных потребностей, кроме прямой [3, с. 209].

Таким образом, за последние несколько лет органы государственной власти различных стран существенно активизировали деятельность, направленную на фильтрацию веб-контента. Вероятно, в ближайшее время эта тенденция сохранится, несмотря на то, что механизмы фильтрации может обойти пользователь, имеющий даже минимальные знания. Фильтрация контента стала в последнее время одной из основных тем, которая активно обсуждается лицами и организациями, выступающими за более жесткое регулирование Интернета, и правозащитными организациями. Именно поэтому отечественные специализированные подразделения по борьбе с киберпреступностью и торговлей людьми должны учитывать эти тенденции и нарабатывать опыт зарубежных стран с целью противодействия этим преступлениям, прежде всего распространению детской порнографии в сети Интернет.

1. Deibert R. Access Denied: The Practice and Policy of Global Internet Filtering [Electronic resource] : MIT Press, 2008. URL: https://dl.acm.org/citation.cfm?id=1349743 (date of the application: 29.01.2019).

2. 2016 World Press Freedom Index: a «deep and disturbing» decline in media freedom [Electronic resource]. URL: https://rsf.org/en/reports/2016-world-press-freedom-index-deep-and-disturbing-decline-media-freedom (date of the application: 29.01.2019).

3. Санакоєв Д. Б. Протидія порнографії в Інтернет підрозділами з боротьби з кіберзлочинністю та торгівлею людьми // Право і безпека. 2011. № 2 (39). С. 207–212.

4. Gesetzesbeschluss des Deutschen Bundestages [Elektronische Ressource]. URL: http://www.doerre.com/jugendschutz/20090619_br_sperrgesetz.pdf (Berufungsdatum: 29.01.2019).